Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Friday, January 13, 2006

Multiparty secure computation

A few years ago I wrote this introduction to a class of cryptographic protocols often called "multiparty secure computation." Wikipedia now also has a good introduction.

The basic idea is to perform a shared yet mutually private computation over the Internet. The computation could be as simple as comparing ages or as complex as an audit or an auction. In this shared computation, the inputs are mutually private, the output shared with all participants, and the privacy of the inputs does not depend on a trusted third party. For example, Alice, Bob, and Charles can each input their ages into the protocol, and the protocol will output a result indicating who is the oldest, without any of them learning the actual age of any other. They can only learn what they can deduce from their own input and the protocol's output.

Here's a good page of links to papers on the subject. There have been some very useful breakthroughs since I wrote on the subject, including orders-of-magnitude improvements in speed and security improvements in terms of how many parties must collude to fake a result or deny a party access to the output.

Posted by Nick Szabo at 11:32 AM

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ► March (11)
  - ► February (10)
  - ▼ January (26)
    - Death by government
    - Two views of Tiananmen Square
    - Free banker to be on Federal Reserve Board?
    - E-gold challenges forfeiture
    - History, property, and security -- update
    - BlackBerry appeal denied
    - Estimating the value of favors
    - Long distance trade in pre-Roman northern Europe

From contracts to money

Google challenges sweeping subpoena for search eng...

What data is on your hotel card key?

Some recent patent news

Professionals sue to stop illegal NSA surveillance...

Trial by ordeal

Laws for the mind police

Multiparty secure computation

More from former NSA spy

Warrantless NSA spying illegal -- more scholars an...

NSA spy doffs his mask

Cowen on currency

Schneier on Project Shamrock

"History and the Security of Property"

E-gold woes

"Imaginary" property

Defensible positions

Shells

► 2005 (44)

Simple theme. Powered by Blogger.